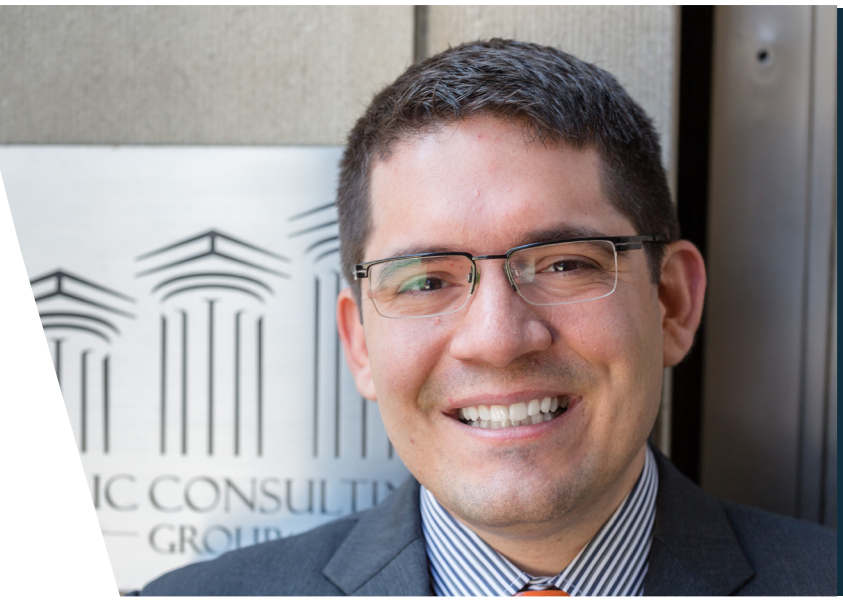
PROFILES IN **CONFIDENCE**

Highlighting information security leaders who are leading the way for confident security programs



MICHAEL BEDFORD

CISO, PUBLIC CONSULTING GROUP

HEADQUARTERS: BOSTON, MA

ANNUAL REVENUE: $35 MILLION

EMPLOYEES: 1,800

A SECURITY LEADER IS A **BUSINESS LEADER FIRST**

While Michael Bedford was still in school he started his own business, an in-home computer repair service. "I learned a lot about being successful in business from that early entrepreneurial effort. I learned the importance of communication, knowing your customer, and providing a good level of service. Ultimately, the business failed, and I learned a lot from that too." This early business experience has impacted his approach to running the security program at Public Consulting Group (PCG). "A security leader is a business leader first," he says. "You have to work as part of the business, not outside of it. You have to have meaningful conversations and interactions with your business counterparts."

CREATING AN OWNERSHIP MENTALITY IS THE BIGGEST **TENET OF SECURITY**

In fact, Bedford believes that communication and collaboration with the company's business leaders and end users has the greatest impact on the success of the security program. "Most security issues involve people, so you have to make sure everyone is working as risk managers at their respective levels," said Bedford. Bedford states that you should know your audience and target your message to them based on their biggest concerns and priorities. "The key is to make sure you get people interested, and make sure they stay invested in security. You want them to understand they are a critical part of the solution. Give folks the right tools and education and they no longer are part of the problem." This bottom-up and top-down approach is proving successful for PCG, as Michael and his team are not only creating a culture of security awareness, but also ensuring that leaders understand security risks in business decisions.

SHOW WHAT YOU **KNOW**

Part of managing security programs involves understanding that there will be ups and downs. Bedford makes sure the rest of the organization hears from the security team when things are going well, not just during an incident or breach. "You have to be able to tell your story, and champion your team. Make sure everyone knows about security's successes, and the value of security, so that when a breach occurs it can be put into context of a larger program, with a trend towards better security." Regular communications from the team also include proactive security education and training for staff on topics that have

> A SECURITY LEADER IS A BUSINESS LEADER FIRST. YOU HAVE TO WORK AS PART OF THE BUSINESS, NOT OUTSIDE OF IT. YOU HAVE TO HAVE MEANINGFUL CONVERSATIONS AND INTERACTIONS WITH YOUR BUSINESS COUNTERPARTS.

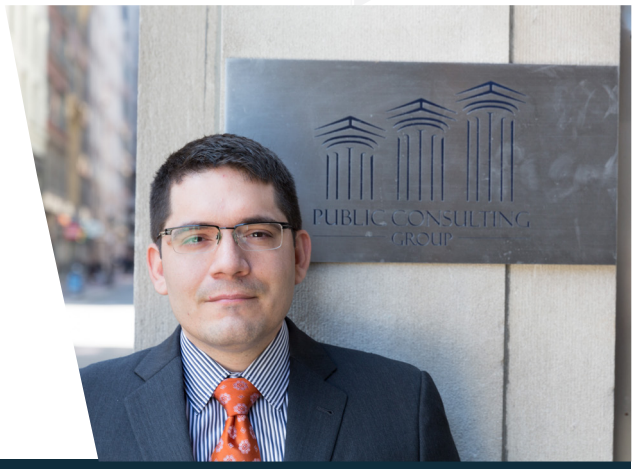
meaning for them both professionally and personally.

ACCEPT THAT CHANGE IS INEVITABLE - SECURITY PROGRAMS ARE LIVING, **NOT STATIC**

"In security, we have to make decisions without all of the information we would like to have. But you have to make decisions and be accountable. Sometimes you get it wrong. If a control is costing manpower or efficiency, without measurably improving security, it's time to change the control," says Bedford. He looks at each part of the program objectively and is always willing to change tactics to support the end goal and business priorities. "Metrics are key to making smarter decisions and not allowing personal biases to get in the way of doing what is necessary to maximize the effectiveness of your security program."

BE FLEXIBLE AND ADAPTABLE - **AGILITY IS KEY**

Bedford believes that companies with confident security programs are built on the strength of confident people. These team members are able to adapt to company culture, become change leaders and champion business goals first and foremost. "You will fail as a CISO if you focus on technology when building your team. We can teach technology and how to support it," says Bedford. "We need to hire people who are focused on problem solving in cost effective and innovative ways. These are the people who are able to adapt to support evolving business requirements and risks. This is what separates ok security programs from great ones."



The Limitations of Frameworks – Security Should Not be a Check-Box Approach

Bedford believes in frameworks, but he cautions against blindly following a list of requirements. "Frameworks are important, but security organizations need to make sure their priorities are focused on mitigating risk. If you can't answer why your organization needs a control, or how it will positively impact the business, then ask yourself why you are doing it? If you were the Board would you support an initiative with no clear business value? Are you checking a box, for the sake of it, or doing effective risk management?"